Section V:	**Physical Security**
Title:	**Environmental Controls Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**May 16, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To provide guidance to the Divisions and Offices of the North Carolina (NC) Department of Health and Human Services (DHHS) to ensure that natural and manmade conditions are addressed and assets are protected from environmental threats.

STANDARD

1.0 Background

Physical security involves providing environmental safeguards as well as controlling physical access to equipment and data. Though the wide variety of premises, building types and building age makes this a challenging prospect, appropriate steps must be taken to ensure the availability of the information infrastructure and in turn the information services it supports through the minimization of environmental risk.

2.0 Environmental Risks

Divisions and Offices shall implement appropriate controls within their facilities to protect physical assets from environmental threats. Environmental threats could hinder or make it impossible to continue normal business operations. Below are a few issues that Divisions and Offices should consider when assessing risk from environmental threats:

- Dust, chemical, particle contaminants
- Electrical system interference
- Explosives damage, electromagnetic radiation
- Fire, smoke, water damage
- Natural disaster, pandemic illness
- Criminal, terrorist, or vandalism activity
- Power outages, HVAC failures
- Issues resulting from strikes, work disruptions or protests

Other threats may need to be addressed based on the entity's unique geographical location, building configuration, neighboring facilities, etc.

3.0 Environmental Risk Management

Divisions and Offices shall take appropriate steps to manage and mitigate the risk of environmental threats to the organization's data and information technology (IT) resources. In accordance with the NC DHHS Security Standards, Administrative Security Standards - Information Security Risk Management Standard, risk assessments shall be performed at all sites where a Division or Office's information is processed or stored to determine the risk from environmental threats, the effectiveness of current controls, and if additional controls are necessary. Below are issues that, at a minimum, shall be considered while assessing risk and developing appropriate mitigation procedures:

- Most file cabinets are not fire, smoke, or water resistant
- Common sprinkler systems are water based and will severely damage paper and electronic equipment
- Densely located electronic and computer equipment will build up and retain potentially damaging heat
- Poor HVAC systems can allow dust and particles to accumulate in electronic equipment fans and vents reducing cooling capacity
- Electronic cabling on floors near equipment can become damaged or build up heat and reduce functional capability
- Data, equipment, or storage sites located near the entrances or exterior of a facility will be more vulnerable to unauthorized access or damage from outside forces

4.0 Environmental Management

Many of the risks from the environmental threats identified above can be addressed through carefully locating equipment and data storage in protected areas and with the use of safety devices and protection controls to ensure that critical systems remain functional and unimpeded operations can continue. Below are issues that, at a minimum, shall be considered while implementing environmental measures to protect data and systems:

- Particulate ventilation systems
- Heat removal and humidification controls
- Compressed inert gas or other approved fire suppression systems
- Heat sensors and smoke alarms
- Raised flooring
- Protective cable conduit
- Water dissipation/drainage systems
- Backup electrical supply

References:

- NC Statewide Information Technology Security Manual, Version No. 01
  - Chapter 05 - Securing Software Peripherals and Other Equipment, Section 02: Cabling, UPS, Printers and Modems
    - Standard 050202 - Managing and Maintaining Backup Power Generators
    - Standard 050206 - Installing and Maintaining Network Cabling

- Chapter 05 - Securing Software Peripherals and Other Equipment, Section 05: Using Secure Storage
  - Standard 050503 - Using Fire Protected Storage Equipment
- Chapter 09 - Dealing with Premises Related Considerations, Section 01: Premises Security
  - Standard 090101 - Preparing Premises to Site Computers and Data Centers
  - Standard 090103 - Ensuring Suitable Environmental Conditions
  - Standard 090109 - Environmental and Other External Threats
- Chapter 09 - Dealing with Premises Related Considerations, Section 03: Electronic Eavesdropping
  - Standard 090303 - Disaster Recovery Plan

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - Physical and Environmental Security Policy

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Security Risk Management Standard